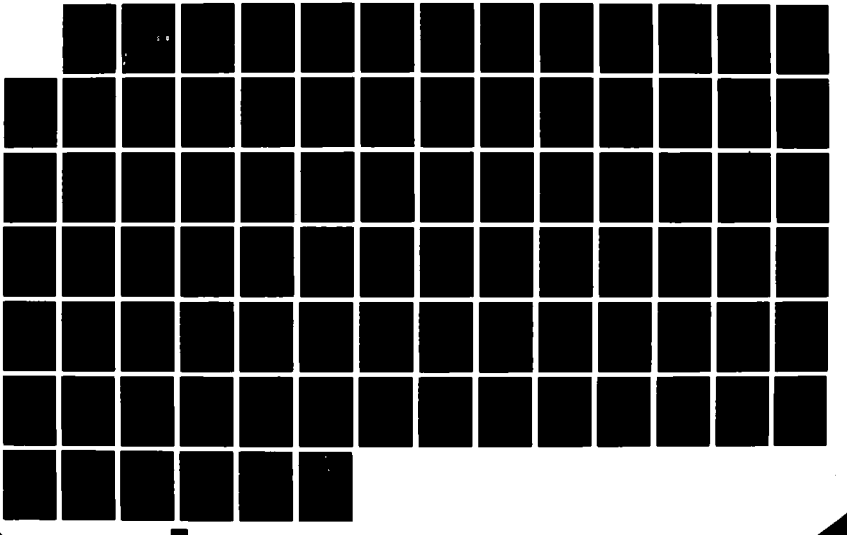
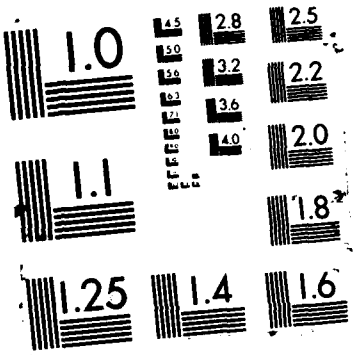
AD-A185 705 A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCE.. (U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH N S BUNCE 1987 1/1

UNCLASSIFIED AFIT/CI/NR-87-80T F/G 15/3 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0

AD-A185 705

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: AFIT/CI/NR 87-80T
2. GOVT ACCESSION NO.: ADA185 705
3. RECIPIENT'S CATALOG NUMBER:

4. TITLE (and Subtitle): A Comparative Analysis of Security Entry Control Programs: Security Forces versus Automated Entry Control
5. TYPE OF REPORT & PERIOD COVERED: THESIS/DISSERTATION
6. PERFORMING ORG. REPORT NUMBER:

7. AUTHOR(s): Neal Steven Bunce
8. CONTRACT OR GRANT NUMBER(s):

9. PERFORMING ORGANIZATION NAME AND ADDRESS: AFIT STUDENT AT: California State University
10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS:

11. CONTROLLING OFFICE NAME AND ADDRESS: AFIT/NR, WPAFB OH 45433-6583
12. REPORT DATE: 1987
13. NUMBER OF PAGES: 70

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office):
15. SECURITY CLASS. (of this report): UNCLASSIFIED
15a. DECLASSIFICATION/DOWNGRADING SCHEDULE:

16. DISTRIBUTION STATEMENT (of this Report): APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

DTIC ELECTE S NOV 0 4 1987 D
cD

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Repo

18. SUPPLEMENTARY NOTES: APPROVED FOR PUBLIC RELEASE: IAW AFR 190-1

LYNN E. WOLAVER 23 Oct 87
Dean for Research and Professional Development
AFIT/NR

19. KEY WORDS (Continue on reverse side if necessary and identify by block number):

20. ABSTRACT (Continue on reverse side if necessary and identify by block number): ATTACHED

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

DTIC FILE COPY

87 10 20 151

A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCES VERSUS AUTOMATED ENTRY CONTROL

Neal Steven Bunce

CAPTAIN

UNITED STATES AIR FORCE

1987

70 pages

MASTER OF SCIENCE

CALIFORNIA STATE UNIVERSITY
SACRAMENTO CALIFORNIA

Accesion For
NTIS CRA&I
DTIC TAB
Unannounced
Justification
By
Distribution /
Availability Codes
Dist | Avail and / or Special
A-1

QUALITY INSPECTED 2

A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCES VERSUS AUTOMATED ENTRY CONTROL

Neal Steven Bunce

CAPTAIN

UNITED STATES AIR FORCE

1987

70 pages

MASTER OF SCIENCE

CALIFORNIA STATE UNIVERSITY
SACRAMENTO CALIFORNIA

Abstract

of

A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCES VERSUS AUTOMATED ENTRY CONTROL

by

Neal Steven Bunce

Statement of Problem

Standard security forces providing entry control to high security areas have often been proven ineffective in their performance. Frequently, they have been plagued by successful unauthorized entries. Automated Entry Control Systems are often being bought, and installed as more efficient alternatives to the traditional security force application. This study attempts to focus on the inherent strengths or weaknesses of each program, as applied, by comparing their essential elements.

Sources of Data

There were three categories of literary sources surveyed in this study. First, a review was conducted of literature relevant to human performance, physiology, psychology, and the biology of work. Next, information on security problems, systems, and technology was examined. Last, writings centered on machine capabilities and efficiency were reviewed.

Conclusions Reached

The elements of both entry control programs were compared and found to be vastly dissimilar. Primarily, automated entry systems provide a level of objective machine consistency that cannot be duplicated by human beings. Inherent human physiological and psychological deficiencies, brought about by the very nature of the job in question, cause a breakdown in efficiency. (Thesis).

Committee Chair's Signature of Approval Thomas Phillips

BIBLIOGRAPHY

Books

Amber, George H., and Paul S. Amber. Anatomy of Automation. Englewood Cliffs: Prentice-Hall, 1962.

Berger, David L. Industrial Security. Los Angeles: Security World, 1979.

Brown, Arthur, and Leonard Norton-Wayne. Vision and Information Processing for Automation. New York: Plenum Press, 1986.

Cluley, J. C. Electronic Equipment Reliability. New York: John Wiley & Sons, 1974.

Coleman, John L. The Security Supervisor's Handbook. Springfield: Charles C. Thomas, 1987.

Coverston, David Y. Security Guard. Ocala: Security Seminars Press, 1986.

Cunningham, John E. Security Electronics. Indianapolis: Howard W. Sams & Co, 1977.

Dummer, G. W. A., and N. Griffin. Electronic Equipment Reliability. New York: John Wiley & Sons, 1960.

Fisher, A. James. Security for Business and Industry. Englewood Cliffs: Prentice-Hall, 1979.

Grandjean, E. Fitting the Task to the Man. London: Taylor & Francis Ltd, 1981.

Healy, Richard J. Design for Security. New York: John Wiley & Sons, 1968.

Luke, Hugh D. Automation for Productivity. New York: John Wiley & Sons, 1972.

Paine, David. Basic Principles of Industrial Security. Madison: Oak Security Publications Division, 1972.

Pick, Jr., Herbert L., and Elliot Saltzman, eds. Modes of Perceiving and Processing Information. New York: John Wiley & Sons, 1978.

Pronikov, A. S. Dependability and Durability of Engineering Products. London: Butterworths, 1973.

Schultz, Donald O. Principles of Physical Security. Houston: Gulf Publishing, 1978.

Sennewald, Charles A. Effective Security Management. Los Angeles: Security World Publications, 1978.

Shearing, C. D., and P. C. Stenning. Private Security and Private Justice: The Challenge of the 80s. Montreal: The Institute for Research on Public Policy, 1983.

Simonson, Ernst, ed. Physiology of Work Capacity and Fatigue. Springfield: Charles C. Thomas, 1971.

Simonson, Ernst, and Philip C. Weiser, eds. Psychological Aspects and Physiological Correlates of Work and Fatigue. Springfield: Charles C. Thomas, 1976.

Singleton, W. T. The Body at Work. Cambridge: Cambridge University Press, 1982.

Strauss, Sheryl, ed. Security Problems in a Modern Society. Boston: Butterworth Publishers, 1980.

Wathen, Thomas W. Security Subjects. Springfield: Charles C. Thomas, 1972.

Woodruff, Ronald S. Industrial Security Techniques. Columbus: Charles E. Merrill, 1974.

Multivolume Works and Series

Aschoff, Jurgen, ed. Biological Rhythms, Vol. 4 of Handbook of Behavioral Neurobiology. New York: Plenum Press, 1981.

Hockey, Robert. Stress and Fatigue in Human Performance. Wiley Series on Studies in Human Performance, Vol. 3. New York: John Wiley & Sons, 1983.

Howell, William C. Information Processing and Decision Making. Human Performance and Productivity Series, Vol. 2. Hillsdale: Lawrence Erlbaum Associates, 1982.

Jackson, John S., ed. Proceedings of the 1977 Conference on Crime Countermeasures and Security. Office of Research and Engineering Services Bulletin Series, No. 112. Lexington: Ores Publications, 1977.

---. Proceedings of the 1983 Conference on Crime Countermeasures and Security. Office of Research and Engineering Services Bulletin Series, No. 130. Lexington: Ores Publications, 1983.

Warm, Joel S. Sustained Attention in Human Performance. Wiley Series on Studies in Human Performance, Vol. 4. New York: John Wiley & Sons, 1984.

Journals

Austin, Brian B. "Controlling Physical Access From a Central Location." Security Management 25:7 (1981): 86-97.

Bajackson, Richard A. "Examining Access Control Need." Security World 20:9 (1983): 40-41.

---. "The Leading Edge." Security World 23:6 (1986): 32-37.

Bean, Charles H., and James A. Prell. "Personnel Access Control--Criteria and Testing." Security Management 21:6 (1978): 6-8, 45-47.

Beebe, Charlene A. "Planning for Access Control." Security Management 28:1 (1984): 77-78.

Bowers, Don M. "Choosing the Right Card." Security World 23:6 (1986): 42-47.

Cole, John P. "The Battle Over Access." Security Management 27:1 (1983): 18-23.

Fowler, Randall C. "Bringing Biometrics to Access Control." Security Management 28:7 (1984): 36-37.

Hershfield, P. E. "Access Control and Its Impact on Security Considerations." Security World 20:9 (1983): 32-37.

Knott, Stuart. "The ABC's of Access Control." Security Management 31:5 (1987): 84-89.

Menkus, Belden. "A Practical Approach to Office Security." Administrative Management 42:6 (1981): 92-94.

Norman, William P. "Detection by Design." Security Management 28:7 (1984): 41-44.

Ragsdale, William F. "Can Universal Badges be a Reality." Security Management 29:12 (1985): 53-55.

Rosacker, Martha. "The Key to Access Controls." Security Management 29:5 (1985): 51-54.

---. "Access Control Alternatives to Card Systems." Security Management 29:8 (1985): 69-73.

Pease, Paul. "Playing a New Card." Security World 23:3 (1986): 75.

Sako, William J. "Computers and Security A New Management Language." Security Management 28:9 (1984): 20-26.

Warfel, George. "Biometrics Proving Positive." Security World 24:2 (1987): 55-57.

Wenger, Deborah C. K. "Decisions, Decisions . . . Finding the Right Access Control System." Security Management 27:9 (1983): 16-19.

A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCES VERSUS AUTOMATED ENTRY CONTROL

Neal Steven Bunce
B.A., Chapman College

THESIS

Submitted in partial satisfaction of
the requirement for the degree of

MASTER OF SCIENCE

in

CRIMINAL JUSTICE

at

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

Summer
1987

A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCES VERSUS AUTOMATED ENTRY CONTROL

A thesis

by

Neal Steven Bunce

Approved by:

Thomas R. Phelps, Chair

James M. Poland, Second Reader

Date: 27 July 1987

Name of Student: Neal Steven Bunce

I certify that this student has met the requirements for format contained in the Manual of Instructions for the Preparation and Submission of the Master's Thesis or Master's Project, and that this thesis or project is suitable for shelving in the library and credit is to be awarded for the thesis or project.

Thomas R. Phelps, Graduate Coordinator — Date 27 July 1987

Department of Criminal Justice

Abstract

of

A COMPARATIVE ANALYSIS OF SECURITY ENTRY CONTROL PROGRAMS: SECURITY FORCES VERSUS AUTOMATED ENTRY CONTROL

by

Neal Steven Bunce

Statement of Problem

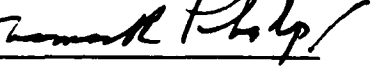
Standard security forces providing entry control to high security areas have often been proven ineffective in their performance. Frequently, they have been plagued by successful unauthorized entries. Automated Entry Control Systems are often being bought, and installed as more efficient alternatives to the traditional security force application. This study attempts to focus on the inherent strengths or weaknesses of each program, as applied, by comparing their essential elements.

Sources of Data

There were three categories of literary sources surveyed in this study. First, a review was conducted of literature relevant to human performance, physiology, psychology, and the biology of work. Next, information on security problems, systems, and technology was examined. Last, writings centered on machine capabilities and efficiency were reviewed.

Conclusions Reached

The elements of both entry control programs were compared and found to be vastly dissimilar. Primarily, automated entry systems provide a level of objective machine consistency that cannot be duplicated by human beings. Inherent human physiological and psychological deficiencies, brought about by the very nature of the job in question, cause a breakdown in efficiency.

Committee Chair's Signature of Approval 

ACKNOWLEDGEMENTS

Several key people contributed immeasurably to this study and I wish to express my sincere appreciation for their efforts.

First, I would like to thank Colonel Lars V. Vedvick, Headquarters Air Force Space Command, for challenging me to pursue my interest in automated entry systems, and actually fathering the idea for this study.

Next, a great deal of thanks are in order for my Thesis Chairman, Dr. Thomas Phelps, who aided in my researching this subject, and who guided me through the project as a whole.

Last, and surely most important, thanks to my wife RuthAnn for her ever present support throughout this wonderful experience.

TABLE OF CONTENTS

	Page
ACKNOWLEDGEMENTS	v
LIST OF FIGURES	viii
Chapter	
1. INTRODUCTION	1
The Problem Stated	1
Purpose of the Study	3
Hypothesis	4
Theory	4
Focus and Limitations of the Study	5
Methodology and Sources Used	6
Definition of Terms	7
Organization of Remainder of Study	9
Endnotes	10
2. REVIEW OF LITERATURE	11
Overview	11
Historical Perspective	12
The Entry Control Environment: Human Considerations	15
The Entry Control Environment: Machine Considerations	26
Endnotes	30

3. THE SECURITY FORCE ENTRY CONTROL PROGRAM . . 34

Overview 34

The Identification Process 35

Enforcement Measures 38

Identity Verification Technique. 39

Communicative Capabilities 40

Organization 41

Endnotes 43

4. THE AUTOMATED ENTRY CONTROL PROGRAM 44

Overview 44

The Identification Process 45

Enforcement Measures 50

Identity Verification Technique. 51

Communicative Capabilities 51

Organization 52

Endnotes 53

5. SUMMARY AND CONCLUSIONS. 55

Summary. 55

Conclusions. 59

Security force performance characteristics. 59

Automated systems performance characteristics. 62

General conclusions. 64

Recommendations for Further Study. 64

BIBLIOGRAPHY 66

LIST OF FIGURES

		Page
1.	Identity Verification Processes	56
2.	Comparison of Man and Machine Capabilities.	63

CHAPTER 1

INTRODUCTION

The Problem Stated

Entry control being provided for high security areas requires a consistency of application without deviation. Absolute identity verification, when possible, has been the governing concept for entry control virtually since its inception. Security forces that have traditionally handled the entry control function have frequently been proven ineffective in their performance of the task. They have continuously been plagued by failures in the form of successful unauthorized entries by spies, thieves, saboteurs, and security evaluators. Their failures in performance have been perceived as the fault of human beings utilized in a task for which they are physiologically and psychologically unsuitable.[1]

People and their forms of identification must be checked thoroughly, each and every time they attempt to enter high security areas, proving their right and need to enter. Conditions that promote a letdown in this proof positive identification process chance an unauthorized entry. Human beings, in a security force role of establishing identity, are theorized as subject to

multitudes of letdowns. These letdowns are simply due to the nature of the work and the physical and psychological inability of human beings to deal with it.

It is important to consider a single high security area with several entrances, and a population consisting of 500 to 3000 people working inside, which is not uncommon for these types of facilities. One or two security officers monitor each entrance and must process hundreds of people in and out of the area during peak specified time frames. During slow traffic periods, the officers are faced with the problem of little to do. The guards are placed in the position of trying to check large numbers of employee identities, process visitors, and otherwise comply with organizational security policies for part of their shift, and at other times have little to do but stand around for hours. These tasks, considered difficult by any set of standards, require an ability to shift from inactivity to the utmost level of performance consisting of vigilance and attention to detail[2]--work requirements for which human beings are found to be unsuitable on the basis of available theoretical information, which constitutes an important assumption in this study.

Technological programs developed to perform entry control functions may be perceived as machines, functioning in much the same way as security forces, but with the consistence of machine proficiency. The Automated Entry

Control Systems approach uses all of the currently recognized methods of identifying people now being employed by guards. This approach is designed to work in a totally objective manner, allegedly offering unquestionable certainty in achieving the state of "Absolute Identity," which is the ultimate goal of any entry control program.[3] The concept in this scenario is that such technology would bring to the entry control discipline a much higher probability of detection of unauthorized personnel attempting entry to a given area--a solution that focuses on the idea that machines are significantly more effective in this security application than guards.

Purpose of the Study

The purpose of this study is to compare and contrast the perceived capabilities of both security force and automated entry control programs. Specifically, the study will examine the strengths or weaknesses of both applications in a systematic manner, attempting to identify the best program in terms of effectiveness. The study will attempt to supplement theory with pertinent practice theory which clearly identifies the most effective program. Comparison of these two particular entry control programs is feasible, because both security forces and automated entry systems use the same standardized approach to establish the identity of personnel authorized in an area.

Hypothesis

Theorizing about the effectiveness of the entry control programs under study has promoted the establishment of a hypothesis that supports a comparative analysis approach to this research. The hypothesis is stated as follows:

> Human physiological and psychological limitations will make security forces, performing entry control functions, considerably less effective in the detection of unauthorized entry attempts than automated entry control systems.

This hypothesis establishes itself as requiring not only efficiency data on each program, but also calls for rationale explaining the manner in which the human method is inherently ineffective. It was structured to lend itself to a fact-finding examination of both human and machine conditions in relation to this specific work environment. It projects the search for pertinent facts, an analysis and logical explanation for all evidence found, and the development of a reasonable pattern of support for the conclusions reached.

Theory

The theories or assumptions promoting the hypothesis stated above focus on the perceived benefits attainable from the application of technology to the task of entry control. These theories or assumptions suggest that security forces are subject and/or susceptible to unauthorized entries, and that there will always be the

skilled infiltrator who often passes through entry control points with only a minimal check of identity.

The major idea developed in this thesis is that automated entry systems can significantly increase the probability of detection of any unauthorized individual attempting entry into a high security area. An increase in security capability ensures better protection of business assets and those of the government, where the very destiny of the nation might be involved.

Focus and Limitations of Study

This study focuses on basic similarities, differences, weaknesses, and strengths of the two entry control programs under analysis. It will review human and machine considerations in relation to the type of work in question, and at those elements within the entry process such as credentials, identification numbers, and physical characteristics. These will be isolated for analysis and then compared in relation to how each entry program handles the verification, identification task. Thus, a specific comparison and subjective analysis of these factors will be accomplished, highlighting specific areas in which there are notable differences. The study will only look at each program as it is maximally applied.

This study will be limited to the review of the relevant, existing literature. It is not the intention of this research to evaluate or determine the quality of each

entry control program through actual side-by-side testing of the systems. Neither is it intended to deal with other philosophical issues or controversies centered on the quality of entry control currently being provided to high security areas.

Methodology and Sources Used

Primarily, the thrust of this study is a comparison of the application, and effectiveness level of both the security force and automated entry control programs. It moves toward this end by first addressing the relevant literature detailing human and machine design considerations within the entry control environment. Secondly, the study will analyze the elements of each program's entry control process, establishing how they are put together and utilized. Finally, the facts on each system will be compared and analyzed in a point-by-point fashion that will either justify or deny the broad hypothesis mentioned earlier.

There were three categories of literary sources used in this study. First, a review was conducted of literature relevant to human performance, physiology, psychology, and the biology of work. Second, information on security problems, systems, and technology was examined. Last, writings directed at machine capabilities and efficiency were reviewed.

Definition of Terms

Entry Control. The procedure used to positively verify the identity/authority of each person seeking entry to an area where entry is restricted.[4]

Security Forces. Those forces consisting of men and women trained, equipped, and utilized to provide security in a given situation or environment. Some of their specific functions are: law enforcement, and the protection of resources (high value assets, weapons systems, classified information, etc.).

Automated Entry Control Systems (AECS). Sometimes referred to as Access Control Systems, they are machine systems designed to positively control, monitor, display, and record the process of entry into areas under their control. These systems use all three currently recognized methods of identifying people. Authorized persons must possess identification credentials, they must know something (their social security number, etc.), and they must be the right person as demonstrated by certain unique physical characteristics.[5]

Credentials/Cards/Badges. Forms of identification carried by the individual. Created to form one means of establishing identity/authority of a person to gain entry to a specified area. Either presented to security force members, or read by automated systems at the area entry point. Contain administrative and/or personal information

on the holder that can be scanned by either security forces, or electronically by automated systems, depending on the application.[6]

Personal Identification Number (PIN). It is a memorized number unique to the credential holder. Either stated to the security force member, or entered on a keypad electronically in automated systems.[7]

Biometric Identification. A means of positively identifying a person through the evaluation of a unique physical characteristic. Done either by a security force member (personal recognition), or through an electronic device (part of an automated system).[8]

Entry Control Booth/Portal. A mantrap housing a specific electronic processing component of an automated entry system (such as the biometric identification device). Positioned at the entrance to an area, it locks the entrant inside, once entered, allowing exit from the trap to the area' s secure side only after entry validation.[9]

Central Processing Unit. The central processor is the heart of the automated system. It is a computer (micro or mini processor) that runs, controls, and monitors the entire system. Comparable, from a parallel standpoint, to the brain of the security force member.[10]

Fixed Post. A security force member assigned station or position for duty. Fixed in this sense means not being able to move from this exact location (stationary).

Template. A gauge or pattern, as a thin metal plate, used in making or copying something accurately.

CCTV. Closed circuit television.

Organization of Remainder of Study

The remainder of this study is divided into four chapters. The relevant literature concerning both human and machine capabilities is reviewed in Chapter 2. This chapter details the literature specifically directed toward human and machine consideration in relation to the entry control environment.

The composition and operation of the security force entry control program is examined in Chapter 3. The examination will focus on the actual process of establishing authority and identity used in this program.

The actual setup, application, and use of automated entry control systems is the subject of Chapter 4. In this chapter, the deployment, and use of an automated entry system in a given area is explored.

Last, in Chapter 5, relevant data on the two programs will be summarized, emphasizing critical weaknesses or strengths noteworthy in each application. The intent here is to provide a picture of which program is most efficient in accomplishing the entry control mission. Finally, in an effort to move this study to a point of logical conclusion, recommendations are made regarding potential areas for further study in the area of entry control.

CHAPTER ONE

NOTES

[1] Sheryl Strauss, ed., Security Problems in a Modern Society (Woburn: Butterworth Publishers, 1980), 134.

[2] Walton N. Hershfield, "Access Control and Its Impact on Security Considerations," Security World 20:9 (1983): 35.

[3] Strauss, 135.

[4] Strauss, 135.

[5] Charlene A. Beebe, "Planning for Access Control," Security Management 28:1 (1984): 77.

[6] Martha Rosacker, "Access Control: Alternatives to Card Systems," Security Management 29:8 (1985): 69.

[7] Rosacker, 70.

[8] Rosacker, 71.

[9] Richard A. Bajackson, "The Leading Edge," Security World 23:6 (1986): 37.

[10] Hershfield, 36.

CHAPTER 2

REVIEW OF LITERATURE

Overview

A great number of sites or facilities worldwide require some form of entry control. This form of control promotes the ability to allow ingress to persons who have a legitimate right or need to be inside the area or facility. Additionally, this type of control dictates the ability to keep unwanted persons out of an area. A result or consequence of the need for entry control is the demand for a system of identification, in order to decide who is authorized for admittance and who is not.[1]

The implementation of entry control can vary from basic to very complex, depending on the application. An entry system will vary: a lock and key format; a guard checking identification; and the use of computers designed to recognize another person by utilizing machines monitoring credentials, personal numbers, and physical characteristics.[2]

The security offered by such systems is measured by the extent to which the system refuses attempts at invalid entry. Reliability depends on the extent to which the system permits valid entries. The designated user

anticipates that the system will be as reliable as possible, because he does not want to be refused a valid entry attempt. The administrator of the entry control system, on the other hand, hopes to implement a system that is as secure as possible, for it is critical that an invalid entry not be allowed. The goal of entry control procedures is to obtain a system which endeavors to combine the best of security and reliability in a cost effective manner. This goal, however, is difficult to achieve, because nearly all existing systems compromise security and reliability.

The most successful programs are those employing security forces or automated components for entry control. Therefore, it is important to explore the means by which humans and machines interact within the entry control environment in order to maximize their actual protective abilities.[3]

Historical Perspective

A major societal concern of mankind is the securing of property, possessions, and the things important to each person. A common response to this problem, and one that is still heavily relied upon in our contemporary culture, was to place a human being on guard for the sole purpose of protecting property. As technology evolved, primitive locks were developed to do some of the control work previously carried out by the security person. In our

contemporary era, locks have been joined by other types of mechanical, electromechanical, and electronic devices to control entry and provide security for property and possessions. Traditionally, however, the use of people as the method for providing security, and specifically entry control, is still the most frequently utilized approach.[4]

In many cases, the identification of personnel is still considered a human function. Security forces within private industry and all branches of the military, are charged with a responsibility for identifying those people working within and visiting their respective installations. These human forces are considered to be the most flexible method of insuring valid identification while providing a human quality in the execution of security services. This traditional application, while considered essentually effective, is known to have a number of limitations.[5]

The considerable cost of using human beings to recognize and identify people is considered an economic hardship by those paying for these services. It has been estimated that it takes 5.2 to 5.8 security guards to adequately monitor one entrance to an area twenty-four hours a day, seven days a week. This results in an annual reoccurring cost for coverage of only one post which may equal $140,000.00 in 1987 dollars. Historically, the human forces have often been found fallible and making mistakes in the performance of their duties; they have been found,

in some cases, to be guilty of collaborating with an intruder.[6] Such concerns, centering on this human fallibility, have facilitated the search for technologically superior entry control systems which provide a more secure, reliable, and cost effective alternative.

Entry control technology has made significant advances within the previous two years as a result of the cooperative efforts of the government and the private sector in the security field.[7] The Department of Defense has shown an increased involvement in the design, testing, and implementation of computer-based entry control systems. Consequently, since 1983, the United States Government has invested hundreds of thousands of dollars to investigate and report on the various aspects of entry control technology.[8] The results of these investigations, although not available in full to the public, have promoted the perception that automated entry systems increase the probability of detection percentage of unauthorized entries. Additionally, these investigations of entry control technology are resulting in the rapid growth of the entry control industry. J. P. Freeman and Co., Newton, Connecticut, in a forecast report for Frost & Sullivan Inc., New York, predicted that electronic entry control products will be among the fastest growing items over the next five years.[9]

The Entry Control Environment:

Human Considerations

Entry control responsibilities are by nature done on a 24-hour-a-day basis, and are broken down into segments. For human beings this work schedule is known as shift work. This is a work routine impacted by the fact that entry control posts are fixed, promoting minimal movement and static conditions for assigned guards. This situation is further influenced by the simple stress of the identification process when the workload varies according to the numbers moving through the entry points. A number of factors are responsible for the critical performance disadvantages experienced by entry controllers, and compounded by physiological and psychological conditions inherent to human beings.[10]

Biologists and physicians have repeatedly stated that the human being is in a performance state in the daytime, and preoccupied with recuperation and the replacement of energy at night[11]--circumstances that are fundamentally tied to the human perceptions of, and lifelong conditioning to daytime hours, the evening, and periods of sleep. Therefore, the worker will approach his shift period, if it occurs at night, not in a mood for peak performance, but rather in the relaxed phase of his daytime cycle, which is a state of being that is one of the big physiological problems of shift work. This is an issue which is

important in the entry control environment because evening shifts comprise two-thirds of the twenty-four hour rotation of labor in the work place.

Human bodily functions which fluctuate in a 24-hour cycle are called the circadian rhythm [meaning one day].[12] When the normal influences of day and night are omitted, such as in a closed room, a kind of internal clock comes into play.[13] This clock varies in each individual, but usually operates in a cycle of between 22 and 25 hours. The bodily functions most affected by circadian rhythms are sleep, work readiness, and many of the nervous system's involuntary processes such as metabolism, blood pressure, and body temperature.[14] These changes in physiological functions have been found to be associated with detrimental lapses in performance, suggesting that humans may not be ideally suited for this type of work. Systematic studies of men engaged in rotating shifts, by Vokac and Rodahl, in 1974 and 1975, indicate that shift work does place physical and psychological strain on the organism. These tensions center on fatigue, boredom, eating habits [nutrition], and the human ability to process data as in the entry control identification process.[15]

As previously stated, as the hours of the day fluctuate, so do the body clocks of shift workers which create a pattern or cycle causing an alignment with fatigue.[16] The symptoms of fatigue in this setting may

range from slight feelings of tiredness to complete exhaustion.

Individuals, working in shifts, often find themselves weary and physically inhibited, having no desire for either physical or mental effort. These feelings are distressing when opportunities for rest or relaxation are not present.[17] These manifestations of fatigue are presented in a diverse number of ways:

(a) visual fatigue (In the vigilance task of entry control the eyes are used heavily in scanning ID data).

(b) muscular fatigue (This can occur when the entry control work requires prolonged sitting or standing).

(c) general body fatigue or physical overloading of the entire system.

(d) mental fatigue.

(e) nervous fatigue.

(f) chronic fatigue as an accumulation of long-term effects.[18]

All of these different kinds of fatigue, brought on by the human phenomenon of circadian rhythms, initiate reduced performance effectiveness for guards in the entry control environment--irregularities that can appear in any of the following ways:

(a) distaste for work.

(b) sluggish thinking.

(c) reduced alertness.

(d) poor/slow perception.

(e) unwillingness to work.

(f) general decline in both bodily and mental performance.[19]

As fatigue develops, in whatever form, individual performance of duties can become irregular. Such irregularities appear slowly at first, but eventually become accentuated, heavily affecting every phase of the task. Studies conducted by W. Harris, R. Mackie, and F. Lecret, in 1972 and 1976, on occupations requiring sustained vigilance during job performance, indicated that the initial indicators of reduced efficiency appear about four hours into the shift, and become very gross after seven to eight hours.[20] These conclusions confirm that the type of routinized work such as one finds in an entry control arena where identification data is transmitted in an auditory, visual, or tactile fashion, is poorly suited for human beings. This finding is further supported by the inabilities of individuals to react positively to the boredom that is an intrinsic factor in this type of work.

Entry control responsibilities, like those of all vigilance tasks, are extremely tedious by design. Those performing duties in this environment are required to be in a designated area for long time periods in order to confirm the identy of people during the period of their work shift. There is little or no variance in the repetitive tasks and, therefore, this can be characterized as boring work.

Monotony or boredom is perceived by the individual when job related tasks lack diversity.[21] It is usually associated with a repetitive and unchanging environment such as that characterized by the entry control function. In a study done by J. Barmack, in 1937, a conclusion was reached suggesting that the feeling of boredom, attributable to a low level of physiological arousal, can cause depressed or inadequate vital activity.[22] This conclusion, supported by an earlier study on the effects of boredom in industry by S. Wyatt, and J. Langdon, in 1932, indicates that it is reasonable to believe that the condition of boredom is responsible for a greater loss in human output than fatigue.[23]

Experience has shown that certain job related circumstances give rise to boredom:

> [a] prolonged repetitive work that is not very difficult, yet which does not allow the individual to think about other things entirely.
>
> [b] prolonged, monotonous work, calling for continuous periods of vigilance.[24]

These are distinct patterns of work that are synonymous with security duties in general, and, in particular, those of entry controllers--modes or states of work that have been found to lower the output, or energy expanded by the individual on the job, highlighting the contradictory application of using human beings in repetitive, high vigilance tasks--working conditions that are not only

themselves detrimental to positive entry control, but compounded by the personal state of guards performing the function.

Working conditions themselves, in this case, are not the only decisive factors in the boredom problem. Individual or personal factors have a considerable effect on the incidence of boredom, or, to put it differently, on the ability of human beings to withstand boredom. Some of these personal factors are the following:

[a] people in a state of fatigue.

[b] people with low motivation.

[c] people with a high level of education, knowledge, and ability.

[d] keen people, who are eager for a demanding job.[25]

All are personal factors that are either known to affect, or that could affect security forces performing entry control functions--a state of affairs that grows even more dangerous, from a vigilance standpoint, when looking at the unevenness of the traffic flow through entry control points and its effect on the human sensory organs.

The streams of impulses from the sensory organs, such as sight, sound, and touch, either stimulate or slow down the activity of the human being's central nervous system.[26] During periods of peak work requirements, such as heavy traffic through entry points, the central nervous system is usually maintained in a high state of readiness. When

stimuli are few, like those periods when little or no traffic moves through entry points, a reduction in the level of activation of the brain occurs, thereby reducing the functional state of the body as a whole.[27]

Both of these conditions can foster two human reactions, neither of which is satisfactory in a vigilance environment. First, during slow stimulus periods, the human tends to become inactive and much less attentive. A study by D. Hebb, in 1955, emphasized that a lack of sensory stimuli severely impaired human perception and cognition[28]--a condition supported by E. Duffy, in a study conducted in 1962, that associated states ranging from deep sleep to extreme excitement, with levels of human functioning.[29] Second, during periods of intense repetitive stimulation, persons tend to become habituated to the task at hand, where identical stimuli lose their effect and become meaningless, impairing the ability of individuals to digest data and/or signals effectively.[30] This was a factor in human vigilance that was proposed by J. Mackworth, in sequential studies taking place in 1968 and 1969 respectively.[31]

Therefore, entry control security and reliability, in this sense, can be degraded simply as a result of the work environment itself, and the human physiological and psychological reactions to it. This creates an environment that continually tasks security forces in a manner that

actually promotes their marginal performance. A fact that can be further explored, within this context, is the examining of security force nutritional factors [eating habits], and the human ability to visually process and comprehend data.

As with automobiles, the human fuel tank must be filled with the proper fuel to propel the body and mind. When left empty or improperly fueled, the mechanism will malfunction or run badly.[32] In this sense, living organisms, like machines, conform to the law of the conservation of energy and must pay for all of their activities in the form of metabolism.[33] Human beings are a product of what they eat, and it is essential that the necessary elements of nutrition be ingested, at the proper times, to insure the gain of adequate energy needed to accomplish tasks over a period of time.

Eating, if not properly approached, can cause malnutrition or improper nutrition, definitely impairing human performance.[34] Security forces, working in shifts, are subject to eating patterns that are often irregular, brief, and approached improperly. Shift workers, by design, eat at unusual times of the day or night. Their break periods, normally used for food consumption, are subject to the security force supervisor's ability to relieve his people in a timely, systematic manner, a situation that is often affected by the work requirements

on a given shift, and by the availability of excess people used for post reliefs. Additionally, the forces are subject to selecting and eating the food that is available to them at the time. Food sources normally used will be the cafeteria in the area (if one exists), fast food outlets (close by), vending machines, or supplies brought from home. These sets of conditions make the forces susceptible to a number of nutritional liabilities that can hinder their performance.

In studies done by Thiis-Evensen, and A. Aanonsen, in 1958 and 1964 respectively, conclusions were reached that showed that shift workers had significantly more digestive ailments and nervous disorders than those working regular hours.[35] Additionally, these studies indicated that shift workers were more likely to report sickness related to stomach troubles, ulcers, intestinal disorders, and nervous disorders.[36] The reasons determined to cause these disorders and ailments were chronic fatigue and unhealthy eating habits.[37]

Unhealthy eating habits, or the intake of food poor in nutritional value, has proven to be logically linked to nutritional deficiencies and, subsequently, to the deterioration of work performance. Studies done by Crandon, Taylor, and Keys, in 1940, 1945, and 1950 respectively, noted that prolonged periods of deficient diets (those poor in vitamin content or untimely for proper

digestion) promoted weakness, increased fatigability, loss of muscle strength, impaired hand/body reaction speed, and deterioration of intellectual and psychomotor performance.[38] Additional information from these studies revealed that these deficiencies appear after long periods of time (six months to a year or more), and are not felt or perceived immediately by those affected.[39] Documented facts, leading to the supposition that poor eating patterns, like those central to security forces working within the entry control environment, would be conducive not only to lower human functional abilities, but to frequent errors in the entry control process itself, errors that may be compounded by human visual perception and information processing limitations.

The word perception is a relevant term to use when discussing human visual capabilities within the entry control environment, because of the word's association with the process of establishing identity. It means, in the simplest sense, the personal experience of seeing, and interpretation of the data seen.[40] The eyes act as receptor organs, picking up data and transmitting it to the brain for interpretation. Any one of a multitude of factors can influence this action, can inhibit it, creatinging visual perception deficiencies.[41]

The viewing of data (such as that seen on identification credentials) is tied to many physical

features: its contrast, size, shape, color and edge sharpness, and the background against which it is seen [lighting].[42] Additionally, other factors affecting the ability of an individual to detect data are his state of adaptation, his motivation [closely related to fatigue and boredom], visual defects [poor sight, eyestrain, etc.], and intelligence.[43]

A study done by McFarland, Halway, and Hurvich, in 1942, determined that one's visual perception abilities are adversely affected by time, area conditions [lighting, color, etc.], type of objects being viewed [size, shape, etc.], and the number of times the objects were viewed [repetition].[44] Additional studies done by Cogan and Hartridge, in 1939 and 1947 respectively, found that items similar in size, shape, and color, viewed in a repetitive manner, eventually became invisible, in terms of perception, to the individual,[45] a disappearance phenomenon that was deduced as a function of stimulus intensity [number of items being viewed in a compressed time period].[46] These are all unacceptable conditions for entry controllers, since they are tasked to visually process standard identification data in a compressed fashion during peak personnel traffic periods--error promoting conditions that are again magnified by their limited ability to mentally process data and sustain attention to the task.

The rate of presentation of data, or the amount of data to be perceived and interpreted in a period of time, is one of the most important variables affecting the information processing capacity of a human being. Studies by H. Jerison, in 1977, indicate that an increase in the event rate (number of times data inspection occurs) results in substantial reduction in vigilance performance, or, in simpler terms, a reduction in the human ability to comprehend data.[47] It appears that this flaw is created by the human inability to sustain attention in successive discrimination tasks, like those associated with identification checks.[48]

The Entry Control Environment: Machine Considerations

Recent developments in machine technology, especially those centering on electronic devices, have prompted the use of machines in many new surroundings,[49] a fact that has reached fruition in the security arena, where electronic technology is being utilized in the form of area/facility exterior and interior protections systems. These security systems are being chosen for reasons that range from dependability to reliability, and are being widely applied by security managers tasked with entry control (positive identification) responsibilities, a situation being further enhanced by the writing of tough technical specifications

for the systems being purchased, driving industry to respond with consistently better products.

Machine engineering is, on a daily basis, being refined and applied to equipment used in high security areas, equipment demanding precision performance, efficiency, dependability, and reliability.[50] The introduction and use of solid-state components and integrated circuits has increased machine capacity while allowing its cost, allowing for very sophisticated machines at economical prices. These technical wonders are being built to withstand any and all conditions found in the security environment, such as extreme heat, extreme cold, high humidity, wind, dust, and user abuse.[51] Additionally, they are being pressure tested by manufacturers to promote error free sustained operations over long periods.[52]

In the entry control arena, machines created to establish identity have been built to operate with low error rates, power/data loss protection, sabotage resistance, low cost maintenance, vast expandability, and ease of user workability.[53] They are constructed, as are all machines generally, to operate in a totally objective fashion with mechanical proficiency. They are fully automatic in their application, and can be entirely self-acting for long periods of time.[54] In effect, they can monitor their own performance and self-correct specific problems through the design of their programming.[55] They

provide a myriad of other qualities, unique to machines in general, that are perfectly suited for the function of establishing identity, 24-hours-a-day, at entry points.

Machines provide certain qualities to users simply because of their physical makeup. The materials from which they are built are strong, and able to hold up well in most surroundings. Specific design strengths allow them to exert and sustain a force or torque indefinitely or until the device is turned off.[56] Machine elements can be designed with the ability to operate at high rates of speed, promoting quick reactions to any given task. Their accuracy, or the correctness of their actions, is limited only by the error specifications given to manufacturers.[57] Additionally, machines are not subject to fatigue, boredom, workload, or hunger, and can be designed to repeat performance uniformly for extended time periods.[58]

As servants to man, all machines are obedient, faithfully following their programming without resistance. Their judgment is reliable over the narrow range of their programming, and they suffer fault only in flexibility because of specialization.[59] Their size and weight is limited only by design and/or function, and they can be built to conform to any installation requirements. They have been advanced enough to duplicate, in specific ranges, the human functions of sight, hearing, touch, and balance,[60] capabilities further enhanced by recently

developed computer aided machine interfaces, vastly improving machine memory capacity and transaction recall ability.[61] These additional facts about machines promote their application in environments calling for these types of performance characteristics.

Machines, then, seem ideal for routine work requiring precision performance. As such, they appear perfectly suited for use within the entry control environment. As previously detailed, they are not subject to human deficiencies, and can be relied upon to perform in a systematic, repetitive, reliable, and efficient fashion.

CHAPTER TWO

NOTES

[1] Sheryl Strauss, ed., Security Problems in a Modern Society, (Woburn: Butterworth Publishers, 1980), 111.

[2] Strauss, 111.

[3] Strauss, 126.

[4] Walton N. Hershfield, "Access Control and Its Impact on Security Considerations," Security World 20:9 (1983): 32.

[5] John E. Cunningham, Security Electronics (Indianapolis: Howard W. Sams & Co, Inc. (1977), 157.

[6] Cunningham, 157.

[7] Richard A. Bajackson, "The Leading Edge," Security World 23:6 (1986): 32.

[8] Bajackson, 32.

[9] Bajackson, 35.

[10] Donald O. Schultz, Principles of Physical Security (Houston: Gulf Publishing, 1978), 32.

[11] E. Grandjean, Fitting the Task to the Man (London: Taylor & Francis Ltd, 1981), 245.

[12] Jurgen Aschoff, ed., Handbook of Behavioral Neurobiology, 5 Vols. (New York: Plenum Press, 1981), 4:57.

[13] Grandjean, 246.

[14] Grandjean, 246.

[15] Per-Olof Astrand and Kaare Rodahl, Textbook of Work Physiology (New York: McGraw-Hill, Inc., 1986), 516.

[16] Aschoff, 335.

[17] Grandjean, 170.

[18] Grandjean, 171.

[19] Grandjean, 182.

[20] Grandjean, 196.

[21] Robert Hockey, ed., Stress and Fatigue in Human Performance (New York: John Wiley & Sons, 1983), 1.

[22] Hockey, 2.

[23] Hockey, 6.

[24] Grandjean, 198.

[25] Grandjean, 198.

[26] Grandjean, 201.

[27] Grandjean, 201.

[28] Hockey, 20.

[29] Hockey, 20.

[30] Joel S. Warm, ed., Sustained Attention in Human Performance (New York: John Wiley & Sons, 1984), 70.

[31] J. F. Mackworth, "Vigilance Arousal and Habituation," Psychological Review 75 (1968): 309.

[32] Astrand, 524.

[33] Astrand, 524.

[34] Astrand, 538.

[35] Grandjean, 253.

[36] Grandjean, 253.

[37] Grandjean, 254.

[38] Ernst Simonson, ed., Physiology of Work Capacity and Fatigue (Springfield: Charles C. Thomas, 1971), 401.

[39] Simonson, 401.

[40] W. T. Singleton, ed., The Body at Work (Cambridge: Cambridge University Press, 1982), 299.

[41] C. H. Bedwell, "The Eye, Vision and Visual Discomfort," Research and Technology 4 (1972): 151.

[42] Singleton, 314.

[43] Singleton, 314.

[44] Ernst Simonson, ed., Psychological Aspects and Physiological Correlates of Work and Fatigue (Springfield: Charles C. Thomas, 1976), 157.

[45] Simonson, Psychological Aspects, 158.

[46] Simonson, Psycholcgical Aspects, 158.

[47] R. Mackie, ed., Vigilance: Theory Operational Performance and Physiological Correlates (New York: Plenum, 1977), 8.

[48] Warm, 74.

[49] J. C. Cluley, Electronic Equipment Reliability (New York: John Wiley & Sons, 1974), 1.

[50] Cluley, 2.

[51] Cluley, 2.

[52] Cluley, 2.

[53] Belden Menkins, "A Practical Approach to Office Security," Administrative Management 42 (1981): 92.

[54] George H. Amber and Paul Amber, Anatomy of Automation (Englewood Cliffs: Prentice-Hall, 1962), 6.

[55] Amber, 7.

[56] Amber, 188.

[57] Amber, 188.

[58] A. S. Pronikov, Dependability and Durability of Engineering Products (London: Butterworths & Co, 1973), 7.

[59] Amber, 188.

[60] Amber, 189.

[61] William J. Sako, "Computers and Security," Security Management 28:9 (1984): 22.

CHAPTER 3

THE SECURITY FORCE ENTRY CONTROL PROGRAM

Overview

Security entry control programs, as referred to in this study, equate to positive personnel identification and control systems, established and maintained in order to preclude unauthorized entry, and facilitate authorized entry to high security areas. In the security force entry control program this task is accomplished by human beings. Their main concern here is to protect property or information from theft, damage, and destruction. There are primarily four groups in the United States who specialize in providing this type of protection. They are:

(a) Military police or security forces (includes all branches of the services and related groups such as the national guard, and state militias).

(b) Department of Defense security or police forces.

(c) Contract and/or private security forces.

(d) Federal, state, and local law enforcement agencies.[1]

They establish the identity of an individual through the use of identification cards or badges (credentials), identification codes (data known to the individual such as

a social security number, etc.), and personal recognition (knowing the person, or comparing physical features against a picture). They are assisted in this task by access lists, prepared by those in control of the facility or area, which catalogue all those people authorized entry privileges. Through these procedures, the security forces hope to achieve the goal of establishing a simple, understandable, and workable identification and control system, using man as the key verification element in the process.

The Identification Process

Security forces use identification cards or badges as their primary tool in establishing identity.[2] These credentials aid them in the control and movement of personnel into, within, and out of specific areas or facilities.[3] The credentials are read (scanned in most cases) by force members charged with entry point duties, who look for specific pieces of information that prove both the credential's or credential holder's authenticity. Information found on these types of credentials will vary, but normally will include the following:

(a) Designation of the various areas where identification cards or badges are required.

(b) Photograph of the holder.

[c] The name, social security number, date of birth, height, weight, eye and hair color, organization, and signature of the holder.

[d] Place of issue.

[e] Any other codes, etc., that tie the credential and holder to the area.

[f] Special design for visitors, including the bearer's name, areas to which entry is authorized, visit time limit, signature, photograph if possible, and information stating if the individual can move alone or must be accompanied by permanent party personnel.[4]

The security force entry controller has the responsibility to review the relevant information on the credential and establish its validity. Once this is accomplished, the credential is returned to the holder for open display on his or her person. This is usually done by means of a clip or chain allowing the credential to be worn outside the clothing. The piece of identification must be able to be seen and distinguishable from a distance, so that security officers or other employees can continuously check people for its possession from across the room, down a hallway, or through a doorway.[5] Credentials used in this manner are sealed inside a cover of clear plastic in order to prevent tampering or forgery. Additionally, both credential issuance and the control of materials used in construction of credentials are security force responsibilities. All forms of this type are issued as controlled items, and

their loss, theft, or mutilation is required to be reported to security forces in a timely manner for appropriate action.[6]

In addition to the basic credential check, security force entry controllers have several backup options available to them for identity verification. First, they can ask personnel for supporting identification in the form of a driver's license, or social security card, that can be used for comparisons of personal data. Second, they can check area entry lists that name, in alphabetical order, all permanent party personnel authorized to enter a designated site for which they are responsible. In the case of visitors, entry lists are prepared in conjunction with known visitor requirements, usually 24 hours in advance. These lists are submitted to the security forces by the organization that owns or operates the facility or area in question. Third, the guard can use personal recognition as a means of granting entry. The idea here is that security forces, having worked an entry position for extended periods of time, develop the ability to recognize those authorized people working in the area simply through repetition. They begin to know, by sight, specific numbers of employees and other personnel that pass regularly in and out of their entry points.[7] They can also compare the bearer's physical features against the photograph found on the entry credential.

Enforcement Measures

The routine performance of comparing bearers with their identification media is the single most essential part of the security force entry control program. As a consequence of this fact, positive measures are established by security forces to standardize the identification process, and to effectively deal with any deviations from the standard that might arise. These measures normally include:

(a) Security personnel designated for duty at entry control points are charged with staying alert, and using good judgement and tact in their performance. They are issued post instructions specifically detailing their responsibilities on a given post.

(b) Uniform methods of handling and wearing identification credentials are established. Credentials must be removed from the wallet or pocket, etc., and handed to the guard for checking.

(c) Guards make visual hands-on inspections of identification materials presented to them, verifying authority before allowing entry.

(d) Entrances to and exits from high security areas are arranged to force arriving and departing personnel to pass in a single file in front of security personnel.

(e) Maintenance of an accurate written log listing, by number, all credentials, showing the total number, to whom issued, and disposition (lost, mutilated, etc.).

(f) Posting at entry points current lists of lost or invalidated credentials.

[g] Procedures to control visitors entering and moving within the secure area. This includes vendors, suppliers, and those visiting on business, etc.

[h] Security force patrols, working in high security areas, making periodic identification checks of those personnel already inside.

[i] Procedures for armed response to any situation that is interpreted as a possible or probable unauthorized entry attempt.[8]

Enforcement of these measures is the most vulnerable link in this human identification system. Perfunctory performance of duty by security force members in screening individuals attempting entry, and responding quickly to any noted problem, may weaken or destroy program credibility.[9]

Identity Verification Technique

Security force entry controllers note all information relevant to identity verification in an audiovisual fashion. Credentials, entry lists, and human physical features, are all being visually absorbed by an entry controller as the candidate entrant answers questions pertaining to identity in an audible manner. The guard's eyes and ears, acting as receptor organs, pick up the data and transmit it for mental analysis.[10] Once this process of perception, interpretation, and information processing is completed, the guard either grants or denies entry to the individual in question. These audiovisual sensory actions take place every time someone attempts to enter the secure area, and may be repeated hundreds of times by an

entry controller during his tour of duty. The entire identity verification process in the security force entry control program is by human beings using inherent sensory and mental faculties.

Communicative Capabilities

From a communications standpoint, security force entry controllers must be thought of as human alarm systems. Their greatest value is in their ability to sound the alarm in the event of an unauthorized or deviant action, such as a bogus entry attempt. They must be able to communicate information accurately and promptly to other entry controllers, armed response forces, and command/control elements of the security force. They have several means at their disposal to accomplish this task.

The best all-around security force communications device is the two-way radio or walkie-talkie.[11] It provides a hand-held mobile capability, allowing security force members to quickly communicate with each other, the dispatcher, response forces, and command elements. These radios offer security forces the best flexibility because of their adaptability to areas and distance through the use of strategically located transmitters. Additionally, standard land-line or telephone systems are used in fixed post applications like that of the entry controller.[12] Other means of communication range from simple silent

duress alarms to whistles. These forms of communication are designed for use by human beings, and, as such, their performance is tied to human thought and action. They are not automated, and must be manually operated in order to be effective.

Organization

The organization of the security force entry control program is dependent on manpower. The forces required to effectively secure an area or facility are determined by the number of entry points, response force requirements, communication needs, and necessary supervisory positions. Normally, the policy is to use a shift work approach consisting of three 8-hour shifts with the changeovers occurring during non-peak employee/visitor traffic hours.[13] Other human factors need to be considered when organizing a program work force. Allowances must be made for the following issues:

(a) Annual leave and days off.

(b) Training time.

(c) Sickness.

(d) Actual work hours--number of 24-hour posts to man, etc.

(e) Associated equipment requirements.

(f) Pay.[14]

The posts required to provide entry control and supporting security services, coupled with the hours each post is required to be manned, determines the number of

security force personnel needed for application of this program. A standardized table or guide used to determine force size requirements would read as follows:

Hours	+ Days Per Week	= People
24hr/day	7	5.4
"	5	3.8
"	2	1.6
16hr/day	7	3.6
"	5	2.5
"	2	1.0
8hr/day	7	1.6
"	5	1.3
"	2	0.5[15]

These figures are based on personnel needed to work a standard 40-hour work week. As applied, they make allowances for the factors of leave, days off, sickness, and training previously mentioned.

CHAPTER THREE

NOTES

[1] Ronald S. Woodruff, Industrial Security Techniques (Columbus: Charles E. Merrill, 1974), 2.

[2] Donald O. Schultz, Principles of Physical Security (Houston: Gulf Publishing, 1978), 83.

[3] Schultz, 84.

[4] David Y. Coverston, Security Guard (Ocala: Security Seminars Press, 1966), 134-135.

[5] David L. Berger, Industrial Security (Los Angeles: Security World Publishing, 1979), 102.

[6] David Paine, Basic Principles of Industrial Security (Madison: Oak Security Publications, 1972), 113.

[7] Schultz, 85.

[8] Schultz, 88.

[9] Schultz, 85.

[10] E. Grandjean, Fitting the Task to the Man (London: Taylor & Francis Ltd, 1981), 154.

[11] Coverston, 119.

[12] Schultz, 75.

[13] Paine, 167.

[14] Paine, 167.

[15] Paine, 167.

CHAPTER 4

THE AUTOMATED ENTRY CONTROL PROGRAM

Overview

As previously mentioned, security entry control programs are instituted whenever entry to areas or facilities must be limited to only authorized individuals. This is done through a process of establishing the identity and authority of the personnel attempting entry. Within the automated entry control program, this task is accomplished through the use of electromechanical computer controlled devices. These devices perform the functions of establishing entry authorization, personal identification, and identity verification. Such equipment, after being bought and installed, is monitored by very limited numbers of security force personnel.

This program uses an approach in establishing authority and identity that is similar to the security force method. Persons using the system are subject to being screened for identification credentials, supporting personal identification data, and physical identity verification information.[1] However, in this case, the individual seeking entry does not interact with other human beings, but rather with machinery.

The Identification Process

Imagine two people entering a nuclear weapons storage facility where the best in available security protection is needed. Every time they enter, they each individually go through the same process at the entry point. They insert their plastic credentials into a reader, punch their personal identification numbers on a keypad, and enter a portal or booth that immediately locks them inside. Once inside the portal, they each peer into a machine that reads the retina of their eye. If all is correct in each of these operations and the two people are determined to be who they say they are, only then will the inner door of the portal open, granting them entry to the facility.[2]

This security procedure combines several measures of identity to ensure that only authorized persons enter the secure area. They have used a card reader, a keypad, a mantrap booth or portal, and a biometric device that scans a physical characteristic.[3] In addition, each person has had to perform all these actions in a sequence; one of them alone would not have achieved the desired result.

This program employs a system of identifying people that uses standard elements recognized for this purpose.[4] Authorized persons must possess something (a credential) tying them to the area in question, they must know something (a number unique to them), they must be the right person as proven by certain unique physical characteristics

[eyes, etc.], and this information must all be verifiable by an intelligent source dedicated to the task. In the automated entry control program, each of these identification elements has been designed to provide the strongest inherent security characteristics.

Credentials and credential readers are the most visible parts of the automated entry control program. The credentials themselves look like simple credit cards, and can have photographs, written identification data, and other visual bits of relevant personal information on the bearer applied to them. Additionally, they can contain logos, holograms, and other unique identifiers that tie the credential to a specific area.[5] They can be encoded, using a variety of methods, which enables each credential to carry its own specific bits of information for analysis by a credential reader.

Card readers are used to read the encoded bits of information contained within a credential prepared for this purpose. Credentials are read by card readers based upon the type of encoding technology applied. Cards may be read by manual insertion of the card into the reader, or simply by radio frequencies generated by the card and picked up by the reader. Once done, the card reader, tied to a computer, uses computer software to answer important questions pertaining to the credentials authenticity.

Information that can be electronically verified consists of the following:

> (a) Is the card valid? In other words, was it issued by those in control of the facility in question?
>
> (b) Who was this card issued to? (Immediately accesses the data file on the person authorized to bear the card in question).
>
> (c) Is admittance authorized at this particular entrance?
>
> (d) Is admittance authorized at this time of day?
>
> (e) Is admittance authorized on this particular date?[6]

If the read of the credential confirms that it is valid, the system allows the respective entrant to proceed to the next step in the automated entry process. At this point, the credential is worn as a badge for internal monitoring by those inside the area.

The next step in the automated entry operation involves the punching in of a personal identification number on a keypad device.[7] This device is also tied to a central computer as is the card reader. Having already accessed a person's data file from the reading of the credential, the computer then compares the personal identification number entered on the keypad to the one listed in the file in question. If the correct combination of numbers is entered, the system provides the voltage to unlock the door to an entry portal.[8]

Upon closing the door to the entry portal behind themselves, entrants are locked into this mantrap. Once inside, they encounter a biometric identification device that must be worked satisfactorily as the last step in the identity verification operation. These double door chambers allow only one person in at a time, and will not allow the person to exit to the secure side until final authorization is permitted by the computer.[9]

Biometric devices, used as the last entry step in this automated application, operate on an entirely different principle from card readers and keypads: they measure unique physical characteristics to determine whether the person seeking entry is indeed the right one.[10] The preceding steps offered a correct credential and personal identification number, both of which could be obtained through theft or coercion. Biometric identification provides a means to check a facet of a human being's physical make-up that cannot be duplicated, stolen, or coerced.

Many personal characteristics can be measured this way due to major technological advances in this area. Electronic units measuring handprints, fingerprints, voice patterns, or the retina of the eye have been made available for use within the automated entry control program. When an individual enrolls on any of these devices, the unit records data about the trait being measured and forms a

gauge or template that is arranged in the individual file by the computer. When the person later uses the device to gain entry, the new image is compared with that of the template. If the two sets of data are sufficiently similar, the individual is assumed to be who he or she claims to be.[11] This action, as with all of the steps in this automated entry process, requires the extraction, comparison, and determination of data by the system's central computer.

The management of the automated entry control program is handled through the use of a microcomputer. It is normally maintained and operated at a central office by security force members, and is responsible for maintaining the integrity of the program's data base.[12] This computer stores all user information relevant to the secure area, and literally controls all aspects of the entry process. It performs the same functions as the security force member. First, it asks for authorization information to be presented for analysis. Second, it must then decide whether the information presented resembles that which has been distributed for entry, whether the information or identification is adequate, and verify that the individual identified is truly the person whose entry is authorized. Last, having decided whether or not the information or data is adequate, entry is either granted or denied.

Additionally, information on each entry transaction is automatically recorded by the computer.

Enforcement Measures

An automated entry control program, to be effective, depends largely on two factors. First, the integrity and cooperation of the people using the system must be maintained. Second, any attempt to circumvent or bypass the system must be met with an alarm and subsequent response by an armed force capable of neutralizing the problem.[13] Consequently, built-in features or controlling procedures that effectively promote these positive measures are established as integral parts of this entry control process. In an automated approach, these include:

(a) All entrances to and exits from high security areas are arranged to force arriving and departing personnel to pass by and use the system's equipment.

(b) A tailgating feature that prevents two persons from entering at one time, and sounds an alarm automatically when this is attempted.

(c) An anti-passback feature that prevents one person from entering and then passing his credential or entry data back to another who will use it, and sounds an alarm if this is attempted.

(d) A security force member, who maintains surveillance over all entry actions through the computer and CCTV cameras positioned at all entry points, monitors all automatic alarms, and dispatches armed response forces when necessary.

[e] Automated procedures for handling and controlling visitors. Includes vendors, suppliers, and those visiting on business, etc.

[f] Procedures for posting changes to computer, reflecting changes in status of personnel, such as lost or stolen credentials, entry privileges, etc.[14]

Identity Verification Technique

The automated entry control system handles all information relevant to identity verification in an electronic, computerized fashion. Credentials, personal identification numbers, and physical characteristics are all absorbed and validated electronically through the computer's microprocessor. The entire process is handled automatically and objectively by the system, with the credential reader, personal identification number machine, and biometric device acting as the computer's eyes and ears. Creating and manipulating identity files, and monitoring the system, are the only human interactions involved here.

Communicative Capabilities

All electromechanical computer controlled devices communicate with the computer through hard-wire connections. Data transmissions are instantaneous, and anyone attempting to illegally interfere with the communications process is stopped by tamper safeguards, built into each component, that automatically sound an alarm. The only human communications requirements revolve

around the computer monitor and armed response forces being dispatched to alarm situations (done through voice, phone, or two-way radio).

Organization

The organization of an automated entry control program hinges on electromechanical devices, a central computer, and minimal security force personnel. As such, they reduce the number of security force personnel needed, make better use of those employed, and use the dollars saved in guard posts to pay for the system's hardware and programming packages.[15]

Initially, such systems must be purchased, installed, tested, and maintained. They also require security force personnel for monitoring and response functions. Security force personnel that are required would work a shift schedule split for day and night coverage, similar to that explained in the previous chapter. The actual number of guards necessary to support the automated elements would be contingent on the size and features of the area or facility to be secured.

CHAPTER FOUR

NOTES

[1] John S. Jackson, ed., Proceedings of the 1977 Conference on Crime Countermeasures and Security, Office of Research and Engineering Services Bulletin Series, No. 112. (Lexington: Ores Publications, 1977), 7.

[2] Martha Rosacker, "Access Control Alternatives to Card Systems," Security Management 29:8 (1985): 69.

[3] Rosacker, 69.

[4] Donald O. Schultz, Principles of Physical Security (Houston: Gulf Publishing, 1978), 83.

[5] Martha Rosacker, "The Key to Access Controls," Security Management 29:5 (1985): 51.

[6] P. E. Hershfield, "Access Control and Its Impact on Security Considerations," Security World 20:9 (1983): 32.

[7] Rosacker, Access Control, 70.

[8] Rosacker, Access Control, 70.

[9] Stuart Knott, "The ABC's of Access Control," Security Management 31:5 (1987): 88.

[10] Rosacker, Access Control, 71.

[11] Rosacker, Access Control, 71.

[12] John S. Jackson, ed., Proceedings of the 1983 Conference on Crime Countermeasures and Security, Office of Research and Engineering Services Bulletin Series, No. 130 .Lexington: Ores Publications, 1983], 98.

[13] Jackson, Proceedings of the 1977 Conference, 9.

[14] Hershfield, 36-37.

[15] Knott, Page 86.

CHAPTER 5

SUMMARY AND CONCLUSIONS

Summary

False acceptance is, of course, the most crucial issue in the entry control process. Keeping a few authorized employees out of a high security area is of little consequence when compared to the risk of admitting a saboteur, thief, or spy. Good entry control measures are preventative in nature, and the security provided is not in catching the wrongdoer, but through the assurance that he or she will never enter a protected facility. Therefore, an effective control program should be constructed in a manner capable of achieving this goal.

The two security entry control programs reviewed in this study attempt to establish the authority and positive identity of all persons attempting entry, in a reliable, precise, consistent manner. They each aspire to this goal by applying methods that, while similar in their intent, differ tremendously in operation. The workings of these two programs focus diametrically on the use of human beings and electromechanical computer controlled devices as the key elements in their identity verification processes (shown in Figure 1). The value of their approaches point

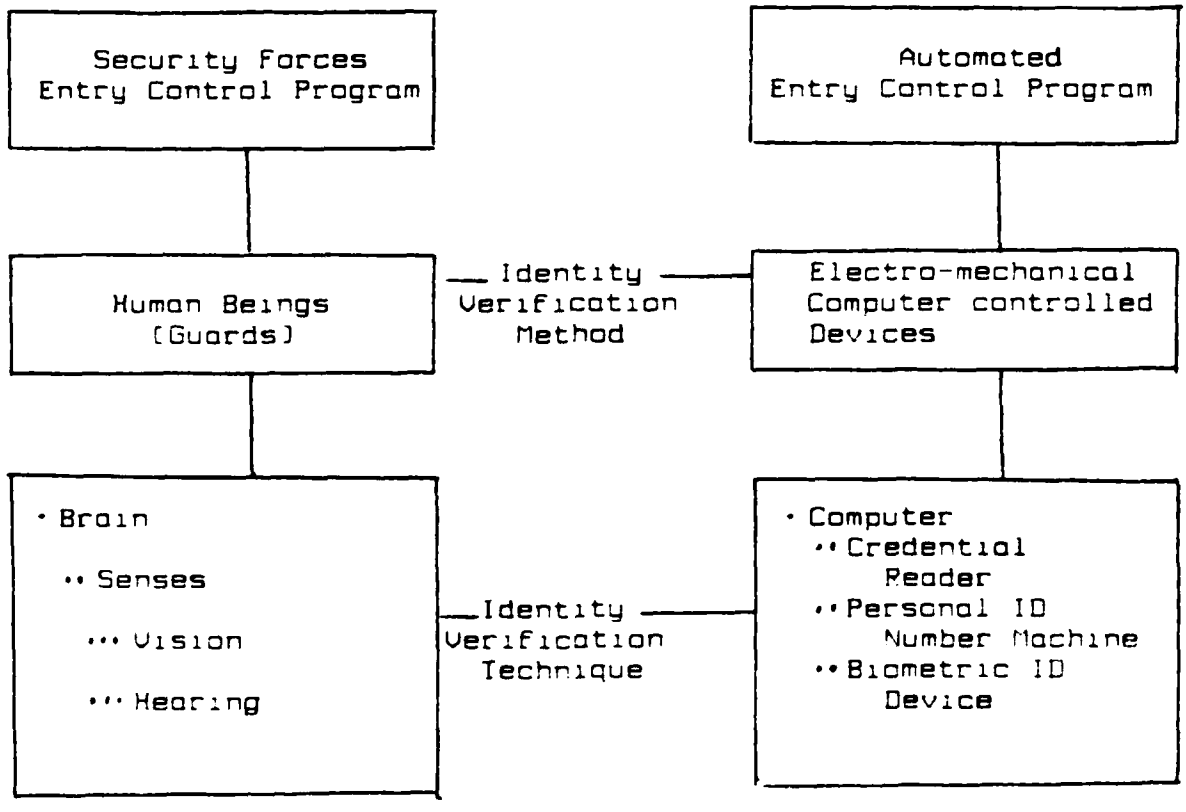


FIGURE 1

Identity Verification Processes

to a person versus machine confrontation, and credibility of each system stands or falls based on their perfunctory performance.

The security force entry control program, using human beings as entry controllers, has been one of the most widely accepted and applied entry control programs in the 1980s. Such a program can supply twenty-four hour surveillance seven days a week, while providing a human quality to the execution of the entry control service. The use of a person in this role, however, does have one major, and seemingly insurmountable, drawback: human fallibility. Humans are susceptable to various physiological and psychological deficiencies that render them virtually incapable of sustaining intense levels of vigilance for any length of time. This inability to sustain the concentration necessary for entry control duty exposes the entry controller to periods of reduction in performance, which places the entire issue of preventing unauthorized entry at risk.

Security force entry controllers are, first and foremost, human beings. As such, their ability to perform any function is limited by biological design. In the case of entry control, the task is not suited to the man. The work schedule includes evening work shifts that adversely affect human performance, lowering output, and leading to ill health which can be classified as occupational. The

repetitive function of inspecting identity is a boring, routinized job, causing a reduction in brain activity and perception. The physical requirements of the job require standing or sitting in one place for prolonged periods of time and this causes fatigue as well as generating deficiencies in alertness, attention, and readiness for action. These job related conditions all make excessive demands on the mind and body, reducing human efficiency.

All of these factors--work shifts, boredom, and fatigue--warrant using an entry control system that operates with maximum efficiency under varying conditions, and which improves the identification process immediately following implementation of procedures. The automated entry control program accomplishes that task through its use of electromechanical components monitored and directed by computer.

The automated entry control program employs machines created to establish identity with low error rates. They are constructed to operate in any environment, regardless of circumstances, providing totally objective machine proficiency. Their actions are fully automatic, with design features incorporating power/data loss protection, sabotage resistance, low cost maintenance, unlimited expandability, computer proven management, and simple user workability. Through inherent qualities, unique to machines, they are perfectly suited for the function of

establishing authority and 24-hours-a-day identification at entry points. They are not subject to fatigue, boredom, workload, or social considerations, and can be relied upon indefinitely with preventative maintenance.

Conclusions

This study was conducted to compare and contrast the capabilities of both security force and automated entry control programs. Specifically, the intent was to outline and examine each program, focusing on design, application, and procedure, as a means of identifying its strengths and or weaknesses (performance characteristics). By consequence, the key identity verification technique employed within each program became the main focus of analysis with the emergence of machine portrayal.

Security force performance characteristics

The entry control activity is, by nature, tedious, repetitive, and performed on a 24-hour-a-day basis. A mixture of work related circumstances generates serious disadvantages for security force personnel performing as entry controllers. These disadvantages are derived from human functions, both physical and mental, that are directly affected by the work routine itself.

The main human functions affected are connected with bodily fluctuations in a 24-hour cycle called the

circadian rhythm. This rhythm controls body states, such as temperature, hormone production, heart rate, blood pressure, adrenalin production, excretion of steroids, mental abilities, and respiratory volume. These states change from low levels early in the morning, to plateaus about midday, to low levels again at night. This pattern has been proven to be related to human activity and individual performance. Entry controllers, working various shifts within a 24-hour period, are subject to these patterns, experiencing changes in their body clock equivalent to the time periods in the day shift. Work shifts, taking place at night, advocate an alignment with fatigue, loss of appetite, digestive troubles, moods of depression, loss of vitality, and general feelings of discomfort, bodily conditions that, upon investigation, were revealed to render an individual incapable of sustaining the high states of accuracy (both visual and audible) required for positive identification of people passing through entry control points. As these bodily conditions develop performance of a task becomes irregular. Various procedures or actions are not followed in the same precise order as they would be by an individual working in harmony with his 24 hour body clock. There are changes in timing, not that all phases slow down but some do, and as a consequence performance becomes erratic. Such irregularities appear at first in short bursts, but

eventually persist, becoming gross and affecting every phase of the task. Information is derived from a number of sources in the entry control environment, and these may be auditory, visual, or tactile in nature. These performance irregularities cause limitations in human perceptual processing abilities. The scanning of fields of display becomes degraded, and frequent lapses in attention may occur. The use of human beings as document or credential checkers involves a high risk because of an inability to sustain visual and auditory discrimination.

Entry control responsibilities are extremely tedious by design. Those performing the function are expected to be positioned in a specified area, for long periods of time, verifying the authority and identity of one person after another. This is routine work at best with little or no variance in the repetitive task boredom that is brought about by a simple lack of sensory stimulating tasks. Entry control work demands a high state of sensory readiness but offers only a low level of sensory arousal. The work by its very design is monotonous a proven condition causing the human mind to become either inactive or inattentive.

Due to both the physiological and psychological factors reviewed it has been proven that human performance in relation to the circumstances in question declines within the first hours of duty. The probability

of detection rate falls off sharply, with periodic lapses in concentration occurring late in the shift of the individual. Human efficiency becomes minimal, providing perfect conditions for unauthorized entry scenarios.

Automated systems performance characteristics

Electromechanical computer controlled equipment performs the entry control function with machine proficiency using the same authority and identity verification procedures as security force entry controllers. They transmit and analyze data through printed circuits using mathematical relationships. They are not limited by brain and muscle tissue and when compared to man outperform him in a myriad of areas (see figure 2).

In their operation within the entry control framework, they are totally objective. They perform the authority and identity verification process the same way every time all of the time. They do not suffer from the types of human failings previously described and are perfectly suited to 24 hour a day operations. These automated components will operate in an extremely reliable fashion as long as they are serviced and powered. They process credentials, code numbers and biometric identification data in a systematic, logical and precise manner unaffected by information load, time of day, or physical location. They have been advanced enough to duplicate and surpass the human functions of

TERM	EXPLANATION	MAN	MACHINE
Strength	The ability to exert and sustain force	Limited Rapidly Diminishes	Limited by design
Speed	Rate at which an action can be accomplished	Slow response time limited ability	fast
Accuracy	Correctness of action	Subject to errors	
[illegible]	Precision of action	Requires training	
[illegible]	Weariness from prolonged exertion	Readily fatigued	Not subject to fatigue
[illegible]	Load to capacity	Readily Saturated	[illegible] by design
[illegible]	To repeat performance	Poor	[illegible]
[illegible]	[illegible] ed performance is intended	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

interrogation, data analysis, and subsequent response actions, making them ideally suited for [illegible] requiring precision performance.

These facts, as presented by the [illegible] examined in this study, point to a potentially substantial increase in the detection of unauthorized entry attempts through the implementation of an automated entry control program. The noted strengths offered by an automated entry control program support the broad hypothesis [illegible] this investigative study.

General Conclusions

Automated entry control programs [illegible] performance [illegible] systems monitoring model. These [illegible]

[illegible]

Recommendations for Future Study

[illegible]

evidence is still needed on the actual probability of detection ratio each entry control program actually provides on unauthorized entry attempts. This information can only be provided through extensive testing of each program while in operation.

This research would give decision makers, in both the government and private sector, vital information that could be used to create a protection/cost matrix detailing actual protective abilities in relation to program costs. Such information is important when considering that a choice in entry control programs means millions of dollars in expense to tax payers and/or corporations, and determines the type of protection provided critical information or resources. Additionally, this data could persuade those employing the security force entry control program to switch. Changing to an automated program approach would displace existing security manpower, amortizing the cost of the new system, and cutting future security force resource requirements.

BIBLIOGRAPHY

Books

Amber, George H., and Paul S. Amber. Anatomy of Automation. Englewood Cliffs: Prentice-Hall, 1962.

Berger, David L. Industrial Security. Los Angeles: Security World, 1979.

Brown, Arthur, and Leonard Norton-Wayne. Vision and Information Processing for Automation. New York: Plenum Press, 1986.

Cluley, J. C. Electronic Equipment Reliability. New York: John Wiley & Sons, 1974.

Coleman, John L. The Security Supervisor's Handbook. Springfield: Charles C. Thomas, 1987.

Coverston, David Y. Security Guard. Ocala: Security Seminars Press, 1986.

Cunningham, John E. Security Electronics. Indianapolis: Howard W. Sams & Co, 1977.

Dummer, G. W. A., and N. Griffin. Electronic Equipment Reliability. New York: John Wiley & Sons, 1960.

Fisher, A. James. Security for Business and Industry. Englewood Cliffs: Prentice-Hall, 1979.

[illegible] Fitting the Task to the Man. London: Taylor [illegible] 1981.

Healy, Richard J. Design for Security. New York: John Wiley & Sons, 1968.

Luke, Hugh D. Automation for Productivity. New York: John Wiley & Sons, 1972.

Paine, David. Basic Principles of Industrial Security. Madison: Oak Security Publications Division, 1972.

Pick, Jr., Herbert L., and Elliot Saltzman, eds. Modes of Perceiving and Processing Information. New York: John Wiley & Sons, 1978.

Pronikov, A. S. Dependability and Durability of Engineering Products. London: Butterworths, 1973.

Schultz, Donald O. Principles of Physical Security. Houston: Gulf Publishing, 1978.

Sennewald, Charles A. Effective Security Management. Los Angeles: Security World Publications, 1978.

Shearing, C. D., and P. C. Stenning. Private Security and Private Justice: The Challenge of the 80s. Montreal: The Institute for Research on Public Policy, 1983.

Simonson, Ernst, ed. Physiology of Work Capacity and Fatigue. Springfield: Charles C. Thomas, 1971.

Simonson, Ernst, and Philip C. Weiser, eds. Psychological Aspects and Physiological Correlates of Work and Fatigue. Springfield: Charles C. Thomas, 1976.

Singleton, W. T. The Body at Work. Cambridge: Cambridge University Press, 1982.

Strauss, Sheryl, ed. Security Problems in a Modern Society. Boston: Butterworth Publishers, 1980.

Wathen, Thomas W. Security Subjects. Springfield: Charles C. Thomas, 1972.

Woodruff, Ronald S. Industrial Security Techniques. Columbus: Charles E. Merrill, 1974.

Multivolume Works and Series

Aschoff, Jurgen, ed. Biological Rhythms, Vol. 4 of Handbook of Behavioral Neurobiology. New York: Plenum Press, 1981.

Hockey, Robert. Stress and Fatigue in Human Performance. Wiley Series on Studies in Human Performance, Vol. 3. New York: John Wiley & Sons, 1983.

Howell, William C. Information Processing and Decision Making. Human Performance and Productivity Series, Vol. 2. Hillsdale: Lawrence Erlbaum Associates, 1982.

Jackson, John S., ed. Proceedings of the 1977 Conference on Crime Countermeasures and Security. Office of Research and Engineering Services Bulletin Series, No. 112. Lexington: Ores Publications, 1977.

---. Proceedings of the 1983 Conference on Crime Countermeasures and Security. Office of Research and Engineering Services Bulletin Series, No. 130. Lexington: Ores Publications, 1983.

Warm, Joel S. Sustained Attention in Human Performance. Wiley Series on Studies in Human Performance, Vol. 4. New York: John Wiley & Sons, 1984.

Journals

Austin, Brian B. "Controlling Physical Access From a Central Location." Security Management 25:7 (1981): 86-97.

Bajackson, Richard A. "Examining Access Control Need." Security World 20:9 (1983): 40-41.

---. "The Leading Edge." Security World 23:6 (1986): 32-37.

Bean, Charles H., and James A. Prell. "Personnel Access Control--Criteria and Testing." Security Management 21:6 (1978): 6-8, 45-47.

Beebe, Charlene A. "Planning for Access Control." Security Management 28:1 (1984): 77-78.

Bowers, Dan M. "Choosing the Right Card." Security World 23:6 (1986): 42-47.

Cole, John P. "The Battle Over Access." Security Management 27:1 (1983): 18-23.

Fowler, Randall C. "Bringing Biometrics to Access Control." Security Management 28:7 (1984): 36-37.

Hershfield, P. E. "Access Control and Its Impact on Security Considerations." Security World 20:9 (1983): 32-37.

Knott, Stuart. "The ABC's of Access Control." Security Management 31:5 (1987): 84-89.

Menkus, Belden. "A Practical Approach to Office Security." Administrative Management 42:6 (1981): 92-94.

Norman, William P. "Detection by Design." Security Management 28:7 (1984): 41-44.

Ragsdale, William F. "Can Universal Badges be a Reality." Security Management 29:12 (1985): 53-55.

Rosacker, Martha. "The Key to Access Controls." Security Management 29:5 (1985): 51-54.

---. "Access Control Alternatives to Card Systems." Security Management 29:8 (1985): 69-73.

Pease, Paul. "Playing a New Card." Security World 23:3 (1986): 75.

Sako, William J. "Computers and Security A New Management Language." Security Management 28:9 (1984): 20-26.

Warfel, George. "Biometrics Proving Positive." Security World 24:2 (1987): 55-57.

Wenger, Deborah C. K. "Decisions, Decisions . . . Finding the Right Access Control System." Security Management 27:9 (1983): 16-19.

END

12-87

DTIC